CLAIMS

1. Method for matching a number N of data reception equipment (2) with a number M of external security modules (6, 8), each reception equipment (2) being provided with a unique identifier, and each external security module (6, 8) having a unique identifier, method characterised in that it comprises a configuration phase comprising the following steps:

- memorising a list of identifiers of reception equipment (2) in each external security module (6, 8),
- memorising a list of identifiers of external security module (6, 8) in each reception equipment (2),

and a check phase consisting of authorising access to data if the identifier of an external security module (6, 8) connected to a reception equipment (2) is present in the list memorised in this reception equipment (2), and if the identifier of said reception equipment (2) is present in the list memorised in said external security module (6, 8), otherwise disturbing access to said data.

2. Method set forth in claim 1, characterised in that the configuration is used only when the user connects an external security module (6, 8) to a reception equipment (2).

3. Method set forth in claim 1, characterised in that the method also comprises a step in which the

operator transmits a signal to the reception equipment (2) to manage the check phase comprising at least one of the following set values:

- activating the check phase at a programmed date or after a programmed delay,
- deactivating the check phase at a programmed date or after a programmed delay,
- specifying an absolute date (or a delay) starting from which (or after which) the check phase is activated or deactivated,
- cancelling said programmed date (or said programmed delay).

4. Method set forth in claim 1, characterised in that the operator also transmits a signal to the reception equipment (2) containing a message to delete the list of identifiers memorised in the reception equipment (2).

5. Method set forth in claim 1, characterised in that the operator also transmits a signal to the external security module (6, 8) containing a message to delete the list of identifiers memorised in this external security module (6, 8).

6. Method set forth in claim 1, characterised in that the operator transmits the list of M identifiers of the external security modules (6, 8) to a reception equipment (2) through an EMM message specific to said reception equipment (2).

7. Method set forth in claim 1, characterised in that the operator transmits the list of identifiers of N reception equipment (2) to an external security module (6, 8) through an EMM message specific to said external security module (6, 8).

8. Method set forth in claim 1, characterised in that the operator transmits the list of M identifiers of external security modules (6, 8) to a group of reception equipment (2) through an EMM message specific to said group of reception equipment (2).

9. Method set forth in claim 1, characterised in that the operator transmits the list of identifiers of N reception equipment (2) to a group of external security modules (6, 8) through an EMM message specific to said group of external security modules (6, 8).

10. Method set forth in claim 3 or 4, characterised in that the operator supplies said signal message to a reception equipment (2) through an EMM message specific to said reception equipment (2).

11. Method set forth in claim 3 or 4, characterised in that the operator supplies said signal message to a group of reception equipment (2) through an EMM message specific to said group of reception equipment (2).

12. Method set forth in claim 5, characterised in that the operator supplies said signal message to an

external security module through an EMM message specific to said external security module (2).

13. Method set forth in claim 5, characterised in that the operator supplies said signal message to a group of external security modules (6, 8) through an EMM message specific to said group of external security modules (6, 8).

14. Method set forth in claim 3 or 4, characterised in the operator transmits a signal message to a group of reception equipment (2) in a private flow for the check phase, said private flow being processed by a dedicated software executable in each reception equipment (2) as a function of the identifier of said reception equipment (2).

15. Method set forth in claim 1, characterised in that the list of identifiers of external security module (6, 8) is transmitted in a private flow to a group of reception equipment (2) and processed by a dedicated software executable in each reception equipment (2) as a function of the identifier of said reception equipment (2).

16. Method set forth in claim 1, characterised in that the list of identifiers of reception equipment (2) is transmitted to a group of external security modules (6, 8) in a private flow that is processed by a dedicated software in each of said external security modules (6, 8) or in the reception equipment (2) to which each of said external security modules (6, 8) is

connected, as a function of the identifier of said external security module (6, 8).

17. Method set forth in claim 1, characterised in that digital data are distributed in plain text or in scrambled form.

18. Method set forth in claim 17, characterised in that digital data are audiovisual programs.

19. Method set forth in claim 1, characterised in that the list of identifiers of M security modules memorised in a reception equipment (2) is encrypted.

20. Method set forth in claim 1, characterised in that the list of identifiers of N reception equipment (2) memorised in an external security module (6, 8) is encrypted.

21. Method set forth in one of claims 6 to 13, characterised in that the method also includes a mechanism designed to prevent use of an EMM transmitted to the same external security module (6, 8) or to the same reception equipment (2).

22. Method set forth in claims 6, 7, 10 or 12, characterised in that said EMM is in the following format:

```
EMM-U_section() {
table_id = 0x88                          8 bits
section_syntax_indicator = 0             1 bit
DVB_reserved                                  1 bit
ISO_reserved                                  2 bits
EMM-U_section_length                          12 bits
unique_address_field                          40 bits
for (i=0; i<N; i++) {
          EMM_data_byte                       8 bits
          }
}
```

23. Method set forth in claims 8, 9, 11 or 13, characterised in that said EMM message concerns all external security modules (6, 8) or all reception equipment (2) and is in the following format:

```
EMM-G_section() {
table_id = 0x8A or 0x8B                       8 bits
section_syntax_indicator = 0                  1 bit
DVB_reserved                                  1 bit
ISO_reserved                                  2 bits
EMM-G_section_length                          12 bits
for (i=0; i<N; i++) {
          EMM_data_byte                       8 bits
          }
}
```

24. Method set forth in claims 8, 9, 11 or 13, characterised in that said EMM message is specific to a sub-group of external security modules (6, 8) or a sub-group of reception equipment (2) and is in the following format:

```
EMM-S_section() {
```

```
table_id = 0x8E                           8 bits
section_syntax_indicator = 0              1 bit
DVB_reserved                              1 bit
ISO_reserved                              2 bits
EMM-S_section_length                      12 bits
shared_address_field                      24 bits
reserved                                  6 bits
data_format                               1 bit
ADF_scrambling_flag                       1 bit
for (i=0; i<N; i++) {
          EMM_data_byte                   8 bits
          }
}
```

25. Method set forth in any one of claims 1 to 24, characterised in that the reception equipment (2) includes a decoder and the external security module (6, 8) includes an access control card (6) in which information about access rights of a subscriber to digital data distributed by an operator is memorised, and in that matching is done between said decoder and said card (6).

26. Method set forth in any one of claims 1 to 24, characterised in that the reception equipment (2) includes a decoder and the external security module (6, 8) includes a removable security interface (8) provided with a non-volatile memory and designed to cooperate firstly with the decoder, and secondly with a plurality

of conditional access control cards (6) to manage access to digital data distributed by an operator, and in that matching is done between said decoder and said removable security interface (8).

27. Method set forth in any one of claims 1 to 24, characterised in that the reception equipment (2) includes a decoder provided with a removable security interface (8) with a non-volatile memory and designed to cooperate firstly with said decoder, and secondly with a plurality of conditional access control cards (6) and in that matching is done between said removable security interface (8) and said access control cards (6).

28. Reception equipment that can be matched with a plurality of external security modules (6, 8) to manage access to digital data distributed by an operator, characterised in that it includes:

- a non-volatile memory designed to memorise a list of external security modules (6, 8),
- means of verifying if the identifier of an external security module (6, 8) connected to said equipment is present in the list memorised in said non-volatile memory.

29. Equipment set forth in claim 28, characterised in that the equipment includes a decoder and in that the external security module (6, 8) is an access control card (6) containing information about access

rights of a subscriber to said digital data, matching being done between said decoder and said card (6).

30. Equipment set forth in claim 28, characterised in that the equipment includes a decoder and in that the external security module (6, 8) is a removable security interface (8) provided with a non-volatile memory and designed to cooperate firstly with said decoder, and secondly with a plurality of conditional access control cards (6), to manage access to said digital data, matching being done between said decoder and said removable security interface (8).

31. Equipment set forth in claim 28, characterised in that the equipment includes a decoder provided with a removable security interface (8) with a non-volatile memory and designed to cooperate firstly with said decoder, and secondly with a plurality of conditional access control cards (6) and in that matching is done between said removable security interface (8) and said access control cards (6).

32. Decoder that can cooperate with a plurality of external security modules (6, 8) to manage access to audiovisual programs distributed by an operator, each external security module (6, 8) having a single identifier and comprising at least one data processing algorithm, decoder characterised in that it includes:

- a non-volatile memory designed to memorise a list of external security modules (6, 8),

- means of verifying if the identifier of an external security module (6, 8) connected to said decoder is present in the list memorised in said non-volatile memory.

33. Decoder set forth in claim 32, characterised in that said external security modules (6, 8) are access control cards (6) in which information about access rights of a subscriber to digital data distributed by an operator is memorised.

34. Decoder set forth in claim 32, characterised in that said external security modules (6, 8) are removable security interfaces (8) including a non-volatile memory and designed to cooperate firstly with the decoder, and secondly with a plurality of conditional access control cards (6) to manage access to digital data distributed by an operator.

35. Removable security interface designed to cooperate firstly with a reception equipment (2), and secondly with a plurality of conditional access control cards (6), to manage access to digital data distributed by an operator, each card having a unique identifier and containing information about access rights of a subscriber to said digital data, interface characterised in that it includes:

- a non-volatile memory designed to memorise a list of subscriber cards,

- means of verifying if the identifier of a card associated with said interface is present in the list memorised in said non-volatile memory.

36. Interface set forth in claim 35 characterised in that it consists of a PCMCIA card containing a digital data descrambling software.

37. Interface set forth in claim 35 characterised in that it consists of a software.

38. Access control system including a plurality of reception equipment (2) each having a unique identifier and that can cooperate with a plurality of external security modules (6, 8) each having a unique identifier, each external security module (6, 8) containing information about access rights of a subscriber to digital data distributed by an operator, said system also including a commercial management platform (1) communicating with said reception equipment (2) and said external security modules (6, 8), characterised in that is also includes:

- a first module arranged in said commercial platform (1) and designed to generate matching queries,
- and a second module arranged in said reception equipment (2) and in said external security modules (6, 8) and designed to process said queries to prepare a matching configuration.

39. Computer program executable on N reception equipment (2) that can cooperate with M security

modules (6, 8) each having a unique identifier and in which information about access rights of a subscriber to digital data distributed by an operator are stored, characterised in that it comprises instructions for memorising a list of identifiers of part or all of N reception equipment (2) in each external security module (6, 8), and instructions to memorise a list of identifiers of part or all of the M external security modules (6, 8) in each reception equipment (2), instructions to control the identifier of a security module connected to a reception equipment (2) and the identifier of said reception equipment (2), and instructions to prevent access to said data if the identifier of the security module (6, 8) connected to the reception equipment (2) is not present in the list of identifiers previously memorised in this reception equipment (2) or if the identifier of said reception equipment (2) is not present in the list of identifiers previously memorised in said external security module (6, 8).